

Security of distributed-phase-reference quantum key distribution

Tobias Moroder,¹ Marcos Curty,² Charles Ci Wen Lim,³ Le Phuc Thinh,⁴ Hugo Zbinden,³ and Nicolas Gisin³

¹*Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Walter-Flex-Str. 3, D-57068 Siegen, Germany*

²*EI Telecomunicación, Dept. of Signal Theory and Communications, University of Vigo, E-36310 Vigo, Spain*

³*Group of Applied Physics, University of Geneva, CH-1211 Geneva, Switzerland*

⁴*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore*

(Dated: July 25, 2012)

Distributed-phase-reference quantum key distribution stands out for its easy implementation with present day technology. Since many years, a full security proof of these schemes in a realistic setting has been elusive. For the first time, we solve this long standing problem and present a generic method to prove the security of such protocols against general attacks. To illustrate our result we provide lower bounds on the key generation rate of a variant of the coherent-one-way quantum key distribution protocol. In contrast to standard predictions, it appears to scale quadratically with the system transmittance.

PACS numbers: 03.67.Dd, 03.67.Hk, 03.67.Mn

Introduction.— Quantum key distribution (QKD) is on the verge to become a standard tool for secure communications [1]. In its original proposal QKD is based on the transmission of single photons. However, since true single photon sources are not available yet most experimental prototypes and all current commercial products of QKD use weak laser pulses. A main drawback of these systems is that some signals contain more than one photon prepared in the same quantum state. This fact severely limits the distances that can be achieved by these techniques due to the photon number splitting attack [2].

To enhance the performance of practical QKD systems, several approaches have been proposed. One solution is to send a strong reference pulse together with the quantum signals [3]. A second approach is based on the decoy state method, where the transmitter sends states with different intensities [4]. Both schemes provide a secret key generation rate that scales linearly with the system transmittance [3, 4]. A third alternative is to use distributed-phase-reference (DPR) QKD protocols. They differ from standard QKD schemes in that the receiver now performs joint measurements onto subsequent signals, often given in the form of coherence measurements [5, 6]. This approach includes the differential-phase-shift [5] and the coherent-one-way (COW) [6] protocols. In the former, the sender prepares coherent states of equal intensity but modulates their phases; in the COW protocol all pulses share a common phase but their intensities vary. A complete security proof of DPR-QKD in a realistic setting has been missing since many years. Security has only been proven so far against restricted types of attacks [7–9], or assuming the use of ideal single photon sources [10].

In this Letter we present a generic method to prove security of practical DPR-QKD against general attacks. This solves a long standing open question in the field of quantum communications [1]. We illustrate our result by providing non-trivial lower bounds for a variant of

the original COW protocol [11], which maintains all the practical advantages. Our analysis suggests that practical DPR-QKD might not be as robust against imperfections as initially foreseen, *i.e.*, its key rate appears to scale quadratically with the system transmittance.

Security discussion.— The challenge in DPR-QKD is to prove security against general, also termed coherent attacks. Usually such attacks are known to be of no advantage to the eavesdropper (Eve) in comparison to collective attacks by virtue of the de Finetti theorem [12]. This theorem applies, for instance, when the underlying quantum state shared by the legitimate users (Alice and Bob) is permutationally invariant. In standard QKD this is typically ensured by performing simultaneous random permutations on the classical measurement results. DPR-QKD defines however a fixed ordering of the signals by its coherence measurement and, therefore, it is not possible to permute the classical outcomes without destroying vital information [13]. However, such a predicament can be circumvented by grouping the entire signal stream into blocks. More specifically, consider that Alice and Bob group their signals into subsequent blocks of size m , where the length m is optimized for the expected behaviour. When permuting these blocks one preserves the coherence information within them while the information between the blocks is destroyed. Still this is enough to apply the de Finetti argument on the level of blocks. As a result, the state shared by Alice and Bob after distributing a large number mN of signals satisfies $\rho_{AB}^{mN} \approx \rho_{AB}^{m \otimes N}$ and security against collective attacks on these signal blocks implies security against coherent attacks in the original setting.

Suppose that the state shared by Alice, Bob and Eve after transmitting an m block signal is ρ_{ABE}^m . Let us first consider the effect of public announcements by Alice and Bob based on their classical measurement results. This announcement, labelled as v , allows both parties to distinguish between conclusive events that contribute to the

sifted key and inconclusive ones that are discarded. On the level of quantum states this is described by suitable maps $\Lambda_v^A \otimes \Lambda_v^B$. Given an announcement v , that happens with probability $p(v)$, the three parties share the state $\sigma_{\text{ABE},v}^m$ determined by $\Lambda_v^A \otimes \Lambda_v^B(\rho_{\text{ABE}}^m) = p(v)\sigma_{\text{ABE},v}^m$.

For each announcement v one can use a one-way classical post-processing key rate formula [14]. If system \bar{A} denotes a qubit and Alice's raw key is obtained by projecting this system onto the orthogonal states $|0\rangle_{\bar{A}}, |1\rangle_{\bar{A}}$, then a lower bound on the secret key rate is given by $1 - h_2(e_v) - h_2(\delta_v)$. Here h_2 represents the binary entropy, e_v is the symmetrized bit error between the key measurements of Alice and Bob, and δ_v denotes the corresponding error, typically called phase error, when Alice performs a measurement in a mutually unbiased basis and Bob in his other different setting. This last parameter is used to upper bound Eve's knowledge on the sifted key generated by Alice. Note that δ_v does not need to be measured directly, it only needs to be estimated. When Bob's measurements are similar qubit measurements like the ones of Alice then the expression above represents the Shor-Prekill key rate formula [15].

To consider that the output system \bar{A} is a qubit implies that Alice can, at best, distill one secret bit per block. Nevertheless this restriction should not have a significant impact on the key rate in a long distance regime, since Bob observes, if any, most often only one single conclusive event per m arriving signals due to the high losses in the channel (given that m is not too big).

Instead of estimating separate phase errors δ_v , it is often easier to combine all conclusive announcements $v \in \mathcal{V}_c$ into an averaged version. Let $G = \sum_{v \in \mathcal{V}_c} p(v) \leq 1$ denote the total sifted key gain. Then, we have that the secret key rate per block can be bounded by

$$\begin{aligned} R_m &\geq \inf_{\rho_{\text{ABE}}^m} \sum_{v \in \mathcal{V}_c} p(v) [1 - h_2(e_v) - h_2(\delta_v)] \\ &\geq \inf_{\rho_{\text{ABE}}^m} G [1 - h_2(\bar{e}_c) - h_2(\bar{\delta}/G)] \\ &\geq G [1 - h_2(\bar{e}_c) - h_2(\bar{\delta}^{\max}/G)]. \end{aligned} \quad (1)$$

Here one uses concavity of h_2 to lower bound R_m by the averaged (conditional) error rates $\bar{e}_c = \sum_{v \in \mathcal{V}_c} p(v)e_v/G$ and $\bar{\delta} = \sum_{v \in \mathcal{V}_c} p(v)\delta_v$. The last step takes into account that \bar{e}_c and G are observed quantities and that the optimization is attained at the largest phase error $\bar{\delta}^{\max}$ compatible with the obtained data since h_2 increases in $[0, \frac{1}{2}]$.

Phase error estimation.— The main difficulty to compute Eq. (2) is to upper bound the average phase error $\bar{\delta}$. This parameter can be expressed as an expectation value on the original bipartite state $\rho_{\text{AB}}^m = \text{tr}_{\text{E}}(\rho_{\text{ABE}}^m)$ using adjoint maps

$$\begin{aligned} \bar{\delta} &= \sum_{v \in \mathcal{V}_c} p(v) \text{tr}(\sigma_{\text{AB},v}^m F_{\delta_v}) = \sum_{v \in \mathcal{V}_c} \text{tr}[\Lambda_v^A \otimes \Lambda_v^B(\rho_{\text{AB}}^m) F_{\delta_v}] \\ &= \text{tr}[\rho_{\text{AB}}^m \sum_{v \in \mathcal{V}_c} \Lambda_v^{A\dagger} \otimes \Lambda_v^{B\dagger}(F_{\delta_v})] = \text{tr}(\rho_{\text{AB}}^m F_{\bar{\delta}}). \end{aligned} \quad (3)$$

Here F_{δ_v} denote the corresponding phase error operators on the state $\sigma_{\text{AB},v}^m$. Partial knowledge of Alice and Bob about the state ρ_{AB}^m can be parsed as known expectation values $k_i = \text{tr}(\rho_{\text{AB}}^m K_i)$ for certain operators K_i . This means that the search for the maximum phase error $\bar{\delta}^{\max}$ can be cast into the form of a semidefinite program [16],

$$\begin{aligned} \max \text{tr}(\rho_{\text{AB}}^m F_{\bar{\delta}}) \\ \text{s.t. } \rho_{\text{AB}}^m \succeq 0, \text{tr}(\rho_{\text{AB}}^m K_i) = k_i \quad \forall i. \end{aligned} \quad (4)$$

Such special convex optimization problems can be solved efficiently using standard tools to obtain the exact optimum, even for large dimensions.

Available information and its description.— Let us be more precise about which expectation values k_i are known in a prepare and measure scheme, where Alice sends potentially mixed states ρ_i^m with a priori probability $p(i)$. This state preparation can be formulated in an entanglement based version as follows [17]: Alice first creates a source state $|\Psi^m\rangle_{\text{A}_b \text{A}_s \text{B}} = \sum_i \sqrt{p(i)} |i\rangle_{\text{A}_b} |\rho_i^m\rangle_{\text{A}_s \text{B}}$, where $|\rho_i^m\rangle_{\text{A}_s \text{B}}$ denote purifications of the signal states ρ_i^m to a shield system A_s [18]. Afterwards, she measures her bit system A_b in the standard basis, thereby producing the correct signal state at site B which is sent to Bob. Eve transforms the overall source state to the final tripartite state ρ_{ABE}^m with $\text{A} = \text{A}_b \text{A}_s$. On the receiving side, Bob performs a measurement modelled by B_k . As a result, both Alice and Bob observe the expectation values of $|i\rangle_{\text{A}_b} \langle i| \otimes \mathbb{1}_{\text{A}_s} \otimes B_k$. Moreover, since Eve is restricted to interact only with Bob's system, the reduced density matrix $\rho_{\text{A}}^m = \text{tr}_{\text{BE}}(\rho_{\text{ABE}}^m)$ is fixed and directly given by the source state. This information can be added by including expectation values of $T_k \otimes \mathbb{1}_{\text{B}}$, where T_k denotes a tomographic complete operator set on A. Both sets of observables constitute the previously denoted set K_i .

The signal states and performed measurements in practical DPR-QKD are described by operators on an infinite dimensional Fock space of several modes. In order to apply the de Finetti argument [12], and to numerically obtain an upper bound on the phase error using Eq. (4), it is necessary to formulate this problem in a manageable, finite dimensional form. Clearly, system A_b is finite. For Bob's measurements one can employ the squash model argument [19]. Here the real measurement is notionally decomposed into a two step procedure by first applying a map that transforms any incoming signal to a finite dimensional output state on which a specified target measurement B_k is performed afterwards. Since this map can be even given to Eve, its output state only lowers the key generation capabilities of Alice and Bob, and one readily works in finite dimensions. For our simulations we assume that Bob has at his disposal inefficient photon number resolving detectors with state independent dark counts. Also, we consider that only the single photon events within the whole block are finally considered as conclusive. In this case the map outputs either a single

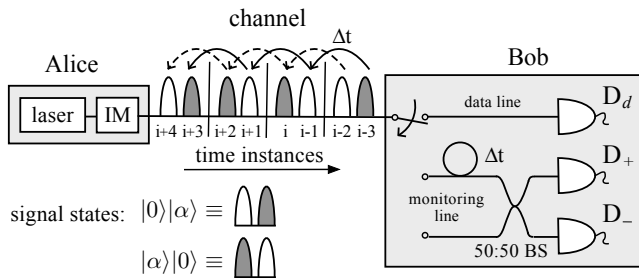


FIG. 1. Schematic description of a COW protocol [11] with an active measurement choice. Bob reads the raw key in detector D_d . Moreover, he uses an optical switch to send some pairs of consecutive pulses to a monitoring line that examines the coherence between even and odd pulses sent by Alice.

photon, measured with the perfect detection scheme, or an auxiliary state that triggers all inconclusive events.

For the shield system A_s one uses only partial information of the reduced state. In the case of phase randomized signal blocks, an example that we consider later, a purification is given by storing the total photon number of the block in the shield system $|n\rangle_{A_s}$. Using only tomography on the subspace spanned by all $n = 1, \dots, n_{\text{cut}}$, together with an ancilla state $|N\rangle_{A_s}$ for all other cases, the shield system can effectively be described in finite dimensions.

Description of the protocol.— To illustrate our results we analyze the security of a variant of the COW protocol [11]. The basic setup is shown in Fig. 1. Alice uses a laser, followed by an intensity modulator (IM), to prepare a sequence of coherent states $|0\rangle|\alpha\rangle$ and $|\alpha\rangle|0\rangle$. On the receiving side, Bob employs an optical switch to distribute each pair of incoming pulses into the data or the monitoring line [20]. The data line measures the arrival time of the pulses in detector D_d and creates the raw key. Whenever Bob sees a “click” in this detector in say time instance i , he decides at random whether to publicly announce a detection event in time instances i and $i+2$ or i and $i-2$. The first case is associated with a bit value “0”, while the second one corresponds to a bit value “1”. If the state sent by Alice in these time instances is $|0\rangle|\alpha\rangle$ ($|\alpha\rangle|0\rangle$) then she assigns to it a bit value “0” (“1”) and tells Bob to keep his result. Otherwise, the result is discarded and does not contribute to the sifted key. Let us illustrate this procedure with a simple example drawn in Fig. 1, and assume that Bob observes a click in D_d in time i . If he announces the pair i and $i+2$, then this result is discarded. Note that in this case Alice sent $|\alpha\rangle|\alpha\rangle$ and hence she cannot infer in which time slot Bob saw a “click”. On the contrary, if Bob reports i and $i-2$, then both parties assign to it a bit value “1”. The monitoring line checks for eavesdropping by measuring the coherence between subsequent even and odd pulses sent by Alice. This is done by interfering adjacent pairs of pulses in a 50 : 50 beamsplitter and measuring the output states in detectors D_+ and D_- .

In the security analysis we assume that Alice and Bob discard coherence information between consecutive signal blocks. Moreover we consider that the sifted key is created only from signals within the same block. To guarantee this, one could discard those detection events where Bob declares time instances that belong to different blocks. Alternatively, one could change Bob’s public announcement slightly. For example, one can reorder the $2m$ possible detection time slots of a given block to form a closed chain with the first and last time instances connected. Now, if Bob observes a “click” in the data line in say the first time slot he announces a detection event in time instances one and three or one and $2m-1$ with equal probability, and similar for the other cases. This strategy preserves the original symmetry in Bob’s announcement and we use it in our simulations.

Simulation.— For simulation purposes, we consider that Bob’s detectors are identical and have a dark count rate of 10^{-7} . The channel model includes an intrinsic error rate of 1% in the data line together with an additional misalignment in the monitoring line that reduces the interferometric visibility to 99%. More details on this channel model and on the adapted security discussion to the COW protocol are given in the appendix. We study two different scenarios: (a) the case where all different m -signals blocks share the same phase, and (b) the scenario where each block is phase randomized. The resulting lower bounds on the secret key rate per pulse, *i.e.*, $R_m/(2m)$, are illustrated in Fig. 2. For comparison, this figure includes as well a lower bound on the secret key rate for a coherent-state version of the standard BB84 protocol [21] with and without phase randomization [22, 23]. For a given total system loss, *i.e.*, including the losses in the channel and in Bob’s detection apparatus, we optimize the lower bound over the respective signal strength α of Alice’s source which is of order 0.1. As expected, we find that case (b) performs better than that where all blocks share a common phase, since the signal states are less distinguishable for an eavesdropper without a global phase. We obtain that the tolerable system loss for the COW protocol is, respectively, ≈ 19.5 dB (a), and ≈ 22.6 dB (b). The bit error and visibility at these cutoff points are, respectively, $\approx 3\%$ and $\approx 96\%$ (a), and $\approx 5.3\%$ and $\approx 93.3\%$ (b). Let us remark that the lower bound with $m = 2$ even holds for threshold detectors [24].

Our simulations reveal that a main limiting factor in DPR-QKD seems to be the dark count rate of Bob’s detectors. For given experimental parameters, there is an optimal finite block size that allows a maximum tolerable total system loss. If one increases the block size further this does not translate into an improved lower bound or distance. This is due to the fact that, in the high loss regime, large sized blocks suffer from a higher dark count probability *per block* than smaller sized blocks, and this reduces the achievable secret key rate. A similar ef-

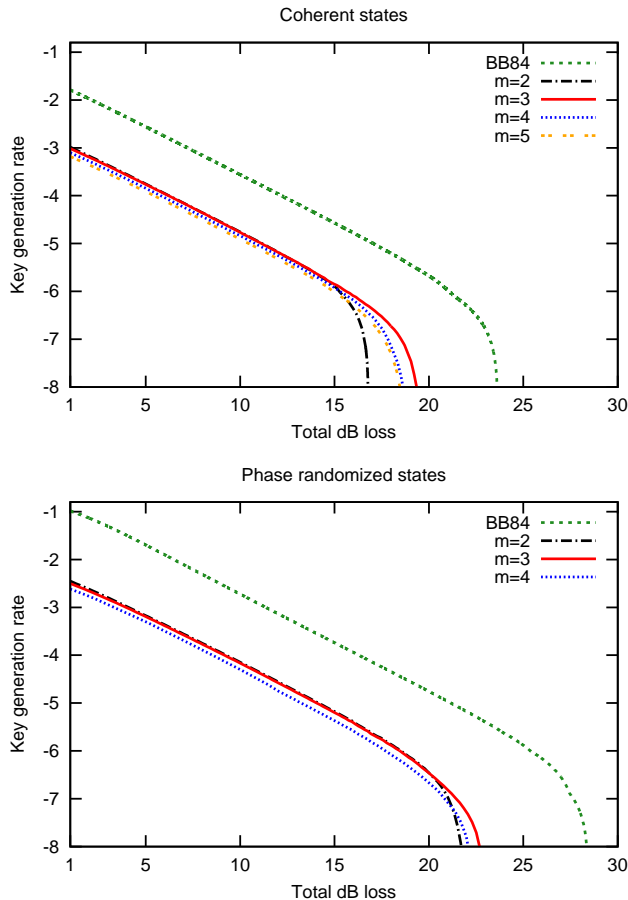


FIG. 2. Lower bound on the secret key rate given by Eq. (2) per pulse on a logarithmic scale (base 10) vs. the total system loss in dB for the COW protocol illustrated in Fig. 1 using signal blocks carrying m bits of information (*i.e.*, $2m$ optical pulses) in the security proof. The upper figure corresponds to the case where all blocks of signals share a common phase, while the lower figure represents the situation where each block is phase randomized. For comparison, we include a lower bound on the secret key rate for a coherent-state version of the standard BB84 protocol [21] with and without phase randomization [22, 23]. We consider three main error contributions: an intrinsic error rate of 1% in the data line, an additional misalignment in the monitoring line reducing the visibility to 99%, and a dark count rate in the detectors of 10^{-7} . Moreover, in the lower figure we assume $n_{\text{cut}} = 2$.

fect was already observed in the security analysis for the differential-phase-shift protocol with true single photon sources [10]. For a dark count rate per pulse of 10^{-7} the optimal block size in the COW scheme turns out to be $m = 3$, *i.e.*, 6 optical pulses. Also, this figure shows that a coherent-state version of the BB84 protocol without decoy states can deliver notably higher key rates per signal than the analyzed COW protocol assuming the same channel model. The reason for this might be threefold: (1) the small optimal block size in the COW scheme; (2) considering blocks, it can be shown that certain multi-photon pulses are completely insecure; (3) most impor-

tantly, while in the BB84 the phase error is measured directly, in the COW protocol it has to be estimated.

Possible improvements.— To further improve the lower bounds shown in Fig. 2 there are several alternatives. Since a main limitation seems to come from dark counts, one may consider security in the fully calibrated device scenario where these errors are not attributed to Eve. As a quantitative bound on the performance of this scenario we investigated the case of a zero dark count rate, in which all key rate bounds shown in Fig. 2 shift by about 3 dB, though the difference between the COW and the BB84 protocol remains. Additionally, one can evaluate different public announcements in a similar spirit like the SARG protocol [25]. We considered different declarations, but unfortunately none of them enhanced the resulting key rate [26]. Another possibility is to include, for instance, an extra monitoring line on Bob's side to additionally check the coherence between subsequent pulses. The state distribution part of this protocol is then very similar to the one of the original COW scheme [6] with an additional decoy signal composed by two vacuum pulses as proposed in Ref. [9]. This hardware change improves the maximum tolerable system loss by about 1 dB.

Another hardware change might be to include additional phase differences in the signal stream, such that the signals states get closer to the one used in a BB84 protocol. Finally, one may ask whether different security techniques might provide better lower bounds. For instance, one could consider more valid detection events per block. This needs however much larger block sizes such that one obtains at all a reasonable fraction of two or more click events in the long distance limit. Another alternative would be to bound the rate by the individual phase errors, *i.e.*, directly using Eq. (1). This could give a benefit if, for example, bits at the boundary are much easier to infer by Eve than bit values originating from events well inside the block. Moreover, it might be of advantage if Eve's information is estimated by using different, possibly not mutually unbiased basis measurements. Here the more general key rate formula of Ref. [14] could be used. Clearly another option would be to abandon the block idea. However even in this case Eve could always attack the signals block-wise. Though a coherence measurement across blocks would then reveal the eavesdropper, any coherence measurement within them would be still fine. Hence when considering only an average visibility this effect will become less and less important. All these alternatives definitely deserve further investigations, but we do not expect a dramatic improvement.

Conclusion.— We have presented a generic method to prove security of practical DPR-QKD against general attacks. With the explicit example of a variant of the COW protocol, we have shown that these schemes are indeed secure for certain distances at given rates. Its performance, however, seems to be less robust against practical imperfections than originally expected.

We would like to thank H.-K. Lo, N. Lütkenhaus, V. Scarani, L. Sheridan and N. Walenta for stimulating discussions about the topic and technicalities, and L. M. Eriksson for comments on the presentation of the paper. T.M., M.C., and L.P.T. especially thank the Group of Applied Physics, University of Geneva, for hospitality and support during their stay at this institution, where parts of this research have been conducted. This work has been supported by the EU (Marie Curie CIG 293993/ENFOQI), the BMBF (Chist-Era Project QUASAR), the National Research Foundation and the Ministry of Education, Singapore, the National Centre of Competence in Research QSIT, the Swiss NanoTera project QCRYPT and the FP7 Marie-Curie IAAP QCERT project.

-
- [1] N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145 (2002); V. Scarani *et al.*, Rev. Mod. Phys. **81**, 1301 (2009).
- [2] B. Huttner *et al.*, Phys. Rev. A **51**, 1863 (1995); G. Brassard, *et al.*, Phys. Rev. Lett. **85**, 1330 (2000).
- [3] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992); M. Koashi, Phys. Rev. Lett. **93**, 120501 (2004); K. Tamaki *et al.*, Phys. Rev. A **80**, 032302 (2009).
- [4] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003); H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005); X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
- [5] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002); K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. A **68**, 022317 (2003); H. Takesue *et al.*, New J. Phys. **7**, 232 (2005); E. Diamanti *et al.*, Opt. Express **14**, 13073 (2006); H. Takesue *et al.*, Nature Photonics **1**, 343 (2007).
- [6] N. Gisin *et al.*, preprint arXiv:quant-ph/0411022 (2004); D. Stucki *et al.*, Appl. Phys. Lett. **87**, 194108 (2005); D. Stucki *et al.*, New J. Phys. **11**, 075003 (2009).
- [7] E. Waks, H. Takesue, and Y. Yamamoto, Phys. Rev. A **73**, 012344 (2006); C. Branciard, N. Gisin and V. Scarani, New J. Phys. **10**, 013031 (2008); Y.-B. Zhao *et al.*, Phys. Rev. A **78**, 042330 (2008).
- [8] M. Curty *et al.*, Quant. Inf. Comp. **7**, 665 (2007); T. Tsurumaru, Phys. Rev. A **75**, 062319 (2007); M. Curty, K. Tamaki, and T. Moroder, Phys. Rev. A **77**, 052321 (2008); H. Gomez-Sousa, M. Curty, Quant. Inf. Comp. **9**, 62 (2009).
- [9] C. Branciard *et al.*, Quant. Inf. Comp. **7**, 639 (2007).
- [10] K. Wen, K. Tamaki, and Y. Yamamoto, Phys. Rev. Lett. **103**, 170503 (2009).
- [11] C. C. W. Lim, N. Walenta, and H. Zbinden, private communication.
- [12] R. Renner, PhD thesis, IJQI **6**, 1 (2008); R. Renner, Nature Physics **3**, 645 (2007).
- [13] Sequential attacks [8, 9] against DPR-QKD also show that its key generation rate differs from the one obtained if one assumes only collective attacks.
- [14] M. Tomamichel, and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).
- [15] P. W. Shor, and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
- [16] L. Vandenberghe, and S. Boyd, SIAM Review **38**, 49 (1996).
- [17] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992); T. Moroder, M. Curty, and N. Lütkenhaus, Phys. Rev. A **74**, 052301 (2006); H. Häsel, and N. Lütkenhaus, Phys. Rev. A **80**, 042304 (2009).
- [18] A shield system refers to an ancillary system that is inaccessible to the eavesdropper. Moreover let us point out that though a single purification $|\rho_i^m\rangle_{A_sB}$ is unique up to local unitary, here one requires that all signals ρ_i^m are purified to the same shield system A_s , which is not unique anymore. While certain collective purifications are clearly better than others, any choice is valid.
- [19] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008); T. Tsurumaru, and K. Tamaki, Phys. Rev. A **78**, 032302 (2008);
- [20] In our simulation we consider, for simplicity, an active measurement choice by Bob. In practice, this can be replaced by a passive optical coupler to select between data and monitoring line, together with an unbalanced Mach-Zehnder interferometer for the coherence measurement.
- [21] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India (IEEE Press, New York, 1984), pp. 175-179.
- [22] D. Gottesman *et al.*, Quant. Inf. Comp. **5**, pp. 325-360 (2004).
- [23] H.-K. Lo, and J. Preskill, Quant. Inf. Comput. **8**, 431 (2007).
- [24] In the easiest setting Bob may want to use threshold detectors, *i.e.*, simple click/no-click detectors, instead of photon number resolving detectors. Using similar arguments like in Ref. [19], it can be shown that, for 2-bit blocks, Bob's measurement apparatus can be described with a squash model and the security analysis applies directly. The resulting secret key rate, however, is almost identical to the case where he uses photon number resolving detectors, only slightly higher in the low loss regime where the probability to obtain a valid detection event is also higher.
- [25] V. Scarani *et al.*, Phys. Rev. Lett. **92**, 057901 (2004).
- [26] In particular, we have examined two further cases. In the first one, whenever Bob sees a “click” in detector D_d in time instance $i \in \{1, 2\}$ ($i \in \{2m, 2m - 1\}$) he always declares a detection event in time instances i and $i + 2$ (i and $i - 2$). Detection events not situated in the border of the blocks are treated as described in the main text. In the second strategy, detection events produced in the border of the blocks are only announced by Bob with probability 1/2. Both methods deliver lower key rates than the one described in the main text.
- [27] M. A. Nielsen, and I. L. Chuang, Quantum Computation and Quantum Information (Cambridge University Press) (2000).

APPENDIX

In this appendix we apply the described security method to the explained version of the COW protocol [11]. In particular, we consider signal blocks carrying m bits of information. Since a single bit comprises two

modes, one has $2m$ different temporal modes described by their creation and annihilation operators a_s^\dagger and a_s , respectively, with $s = 1, \dots, 2m$. We assume that the l -th bit relates to the modes with $s = 2l - 1, 2l$.

Real and assumed measurement description.—At first let us concentrate on the real measurement model M_k^{real} and the way how we describe it in the security part, denoted as B_k in the main text. For the real measurement setup we assume inefficient photon number resolving detectors that suffer from state-independent dark counts. The inefficiency of M_k^{real} is modelled by a global beam-splitter (BS) of transmittance η_{det} located in front of a perfectly efficient scheme, labelled as M_k , that still suffers from dark counts. This is schematically drawn in the first line of Fig. 3. In a second step, one models the efficient scheme M_k as a map Λ_s , sometimes called squashing or filter operation [19], in front of the assumed description B_k . Let us emphasize that the security simulation is valid for any true measurement scheme that can be modelled as a physical map Λ followed by the measurement B_k as shown in the third line of the figure.

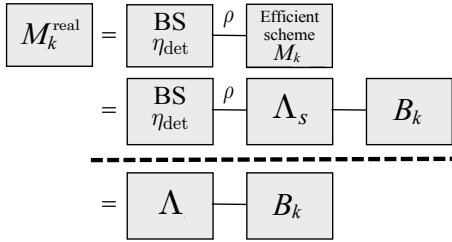


FIG. 3. Decomposition of Bob's measuring device.

There are three different types of outcomes for the so far abstract outcome label “ k ”. For a data line measurement we use d , with $d = 1, \dots, 2m$, to denote a single photon detection in temporal mode d only. The corresponding measurement operator M_d is given by

$$M_d = \epsilon(1 - \epsilon)^{2m-1} |\text{vac}\rangle\langle\text{vac}| + (1 - \epsilon)^{2m} |d\rangle\langle d|, \quad (5)$$

with ϵ representing the dark count probability of Bob's detectors and $|d\rangle = a_d^\dagger |\text{vac}\rangle$. In addition to a data line measurement Bob can also perform coherence measurements on subsequent bits employing the monitoring line. For instance, whenever he tests the coherence between bits l and $l+1$ he effectively mixes the modes $2l-1, 2l+1$ and, at the same time, $2l, 2l+2$. For each pair of modes there are two single photon events, denoted as \pm , that can be distinguished, depending on whether the single excitation is registered in the bright (D_+) or in the dark (D_-) detector. As an outcome label for the coherence measurements we use $k = (c, \pm)$, where $c = 1, \dots, 2m-2$ denotes the first of the two interfering modes. In this case the measurement operators are given by

$$M_{c,\pm} = \epsilon(1 - \epsilon)^{2m-1} |\text{vac}\rangle\langle\text{vac}| + (1 - \epsilon)^{2m} |\chi_c^\pm\rangle\langle\chi_c^\pm|, \quad (6)$$

with $|\chi_c^\pm\rangle = (|c\rangle \pm |c+2\rangle)/\sqrt{2}$. Let us emphasize that in these coherence measurements it is still necessary to check that all other modes are empty. Finally, note that each measurement setting has also other possible outcomes, e.g., “no click” or more than a single photon detection event. All these cases are grouped (via classical post-processing) into a single inconclusive outcome described by M_{inc} .

As the modelled measurement operators B_k we use

$$\begin{aligned} B_d &= |d\rangle\langle d|, \\ B_{c,\pm} &= |\chi_c^\pm\rangle\langle\chi_c^\pm|, \\ B_{\text{inc}} &= |a\rangle\langle a|, \end{aligned} \quad (7)$$

where $|a\rangle$ is the auxiliary state that describes the inconclusive outcome. These measurement operators B_k act on a $2m+1$ dimensional Hilbert space.

Both measurement sets can be made equivalent by an appropriate map Λ_s such that $\text{tr}(\rho M_k) = \text{tr}[\Lambda_s(\rho) B_k]$ holds for all possible states ρ and measurement outcomes “ k ” as schematically shown in Fig. 3. This map Λ_s is given as follows. First one measures the total number of photons n within an arriving block. Whenever one finds $n \geq 2$ one outputs the auxiliary state $|a\rangle$. If $n = 1$ then with probability $(1 - \epsilon)^{2m}$ the single photon state stays untouched, otherwise the auxiliary state is thrown again. Finally, for $n = 0$ the map creates the completely mixed single photon state $\sum_k |k\rangle\langle k|/2m$ with probability $2m\epsilon(1 - \epsilon)^{2m-1}$ and $|a\rangle$ otherwise. This map is physical because we explicitly describe it in terms of measurements and conditional signal state preparations.

Source state and reduced density matrix.—The following discussion provides the source states for both cases of pure or phase randomized COW block signals. These states determine the reduced density matrix ρ_A^m which belongs to the available information.

Let us consider first the case of pure signal states. In the COW protocol analyzed Alice sends to Bob either the sequence $|\alpha, 0\rangle$ or $|0, \alpha\rangle$, with $\alpha \in \mathbb{R}$, depending on whether her raw key bit value is “0” or “1”. Let us start with the scenario where Alice sends to Bob only one bit value, occurring with equal a priori probability. This corresponds to a block size $m = 1$. Then the source state is given by

$$|\Psi^{m=1}\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A |\alpha, 0\rangle_B + |1\rangle_A |0, \alpha\rangle_B), \quad (8)$$

and its reduced density matrix becomes

$$\rho_A^{m=1} = \frac{1}{2} \begin{bmatrix} 1 & e^{-\alpha^2} \\ e^{-\alpha^2} & 1 \end{bmatrix}. \quad (9)$$

Suppose now that Alice sends to Bob m bits according to this scheme. If $i = (i_1, i_2, \dots, i_m)$ denotes the m -bit string being sent and $|\phi_i\rangle_B$ refers to the corresponding

signal state, then one obtains

$$\begin{aligned} |\Psi^m\rangle_{AB} &= 2^{-\frac{m}{2}} \sum_{i \in \{0,1\}^m} |i\rangle_A |\phi_i\rangle_B \\ &= |\Psi^m\rangle_{A_1 \dots A_m B} = |\Psi^{m=1}\rangle_{AB}^{\otimes m}. \end{aligned} \quad (10)$$

In particular, from the last expression one finds that the reduced density matrix ρ_A^m is given by

$$\rho_A^m = (\rho_A^{m=1})^{\otimes m}. \quad (11)$$

Next, let us turn to the case of phase randomized blocks. Since randomizing the phase of a block is equivalent to measuring the total number of photons contained in it, the true signals states are of the form

$$\rho_i^m = \sum_{n=0}^{\infty} \Pi_n |\phi_i\rangle_B \langle \phi_i| \Pi_n = \sum_{n=0}^{\infty} p_\lambda(n) |\psi_n^i\rangle_B \langle \psi_n^i|. \quad (12)$$

Here Π_n stands for the projector onto the n -photon subspace of the $2m$ different modes. The outcome of such a photon number measurement follows a Poisson distribution $p_\lambda(n) = e^{-\lambda} \lambda^n / n!$ with mean $\lambda = m\alpha^2$. The projected n -photon signal states $|\psi_n^i\rangle_B$ can be expressed as

$$|\psi_n^i\rangle_B = m^{-\frac{n}{2}} \sqrt{n!} \sum_{n_1, \dots, n_m} \prod_{l=1}^m \frac{(a_{2l+i_l-1}^\dagger)^{n_l}}{n_l!} |\text{vac}\rangle_B, \quad (13)$$

where the summation runs over all natural numbers n_1, \dots, n_m that satisfy $\sum_{l=1}^m n_l = n$. These states fulfill the relation

$$\langle \psi_n^i | \psi_n^j \rangle = \delta_{n\bar{n}} \left(\frac{m - \Delta_{ij}}{m} \right)^n, \quad (14)$$

with Δ_{ij} being the Hamming distance between the bit strings i and j , *i.e.*, the number of places they differ.

Using the framework of mixed signal states as explained in the main text one must now choose an overall purification of all signal states $|\psi_n^i\rangle_B$. For our simulation we select

$$|\rho_i^m\rangle_{A_s B} = \sum_{n=0}^{\infty} \sqrt{p_\lambda(n)} |n\rangle_{A_s} |\psi_n^i\rangle_B, \quad (15)$$

which can be seen as a coherent storage of the total photon number n in the shield system A_s . Let us remark that this choice satisfies $\langle \rho_i^m | \rho_j^m \rangle = F(\rho_i^m, \rho_j^m)$, with F being the fidelity of mixed states, which is also the maximal possible overlap between two signal states [27]. We find, therefore, that the source state in this scenario is given by

$$|\Psi^m\rangle_{A_b A_s B} = 2^{-\frac{m}{2}} \sum_{i \in \{0,1\}^m} |i\rangle_{A_b} |\rho_i^m\rangle_{A_s B}, \quad (16)$$

with $A_b = A_1 \dots A_m$. This means that the reduced density matrix ρ_A^m , with $A = A_b A_s$, can be expressed as

$$\rho_A^m = \sum_{n=0}^{\infty} p_\lambda(n) \rho_{A_b}^n \otimes |n\rangle_{A_s} \langle n|, \quad (17)$$

with $\rho_{A_b}^n$ given by

$$\rho_{A_b}^n = 2^{-m} \sum_{i,j} \left(\frac{m - \Delta_{ij}}{m} \right)^n |i\rangle_{A_b} \langle j|. \quad (18)$$

In our simulation we only use partial information of the reduced density matrix ρ_A^m . In particular, we transform A_s to \bar{A}_s by making a shield measurement that distinguishes the different photon number cases mentioned in the main text such that one obtains

$$\begin{aligned} \rho_{A_b \bar{A}_s}^m &= \sum_{n=1}^{n_{\text{cut}}} p_\lambda(n) \rho_{A_b}^n \otimes |n\rangle_{\bar{A}_s} \langle n| \\ &+ \sum_{n \notin \{1, \dots, n_{\text{cut}}\}} p_\lambda(n) \rho_{A_b}^n \otimes |N\rangle_{\bar{A}_s} \langle N|, \end{aligned} \quad (19)$$

where $|N\rangle_{\bar{A}_s}$ denotes an auxiliary system for all higher photon numbers. Let us point out that considering the reduced state given by Eq. (19) can be understood as “tagging” the $n = 1, \dots, n_{\text{cut}}$ signal states [22].

Announcement maps and phase operator.—The specific announcements v of the COW protocol can be phrased in terms of appropriate maps Λ_v on the quantum state. Together with a chosen “phase setting” measurement this provides a concrete expression for the averaged phase error operator $F_{\bar{s}}^B$ used in Eq. (3).

As explained in the protocol description, Bob announces two consecutive even or odd time slots where he registered his single photon event. Suppose, for instance, that he announces $v = (2l - 1, 2l + 1)$. These are the first arrival times of the modes associated with bits i_l and i_{l+1} sent by Alice. In such cases, Alice and Bob agree to call the outcome in the first time instance “0” while the later event is “1”. This announcement can be modelled as a filter operation $\Lambda_v^B(\rho) = F_v^B \rho F_v^{B\dagger}$ given by

$$F_v^B = \frac{1}{\sqrt{2}} (|0\rangle_{\bar{B}B} \langle 2l - 1| + |1\rangle_{\bar{B}B} \langle 2l + 1|). \quad (20)$$

If Bob measures system \bar{B} in the standard basis $|0\rangle_{\bar{B}}, |1\rangle_{\bar{B}}$ he obtains the real outcome he has observed. The prefactor $1/\sqrt{2}$ which appears in Eq. (20) takes into account that whenever Bob sees a single photon click in either $2l - 1$ or $2l + 1$ he announces this particular v with just 50% probability, *i.e.*, $F_v^{B\dagger} F_v^B = (B_{2l-1} + B_{2l+1})/2$.

Suppose Bob has actually declared $v = (2l - 1, 2l + 1)$. Then, Alice has to look on her bit string to determine whether she can conclusively infer Bob’s bit value. For that, only her bits i_l and i_{l+1} matter. As shown in Fig. 4, if these two bits are equal it means that she had sent to Bob either two full or two empty pulses. In this scenario,

she cannot infer Bob's bit value and they discard this result. However, if these bits differ then she knows Bob's sifted bit value precisely (in the error free case) and she tells Bob to keep it. Such a conclusive announcement

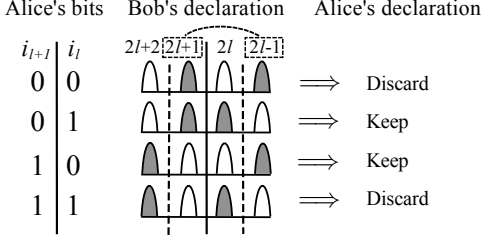


FIG. 4. Announcement choices for Alice given that Bob has declared a detection event in time slots $2l - 1$ and $2l + 1$.

by Alice can similarly be modelled as a filter operation Λ_v^A acting on her qubits l and $l + 1$, *i.e.*, $\Lambda_v^A(\rho_{A_1 \dots A_m}^m) = F_v^A \rho_{A_1 A_{l+1}}^m F_v^{A\dagger}$ with

$$F_v^A = |0\rangle_{\bar{A}} \langle 0|_{A_1 A_{l+1}} + |1\rangle_{\bar{A}} \langle 1|_{A_1 A_{l+1}}. \quad (21)$$

Again a measurement in the standard basis $|0\rangle_{\bar{A}}, |1\rangle_{\bar{A}}$ provides Alice with her real outcomes.

In order to determine the phase error δ_v we assume that both parties perform measurements in the X -basis, *i.e.*, they project the output signals from their filter operations onto the states $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Then, the symmetrized phase error $\delta_v = p(+, -) + p(-, +)$ can be expressed as

$$\begin{aligned} p(v)\delta_v &= p(v) \text{tr} \left[\frac{1}{2} (\mathbb{1} \otimes \mathbb{1} - \sigma_x \otimes \sigma_x) \sigma_{\bar{A}B,v}^m \right] \\ &= \frac{1}{2} p(v) - \frac{1}{2} \text{tr} (\sigma_x \otimes \sigma_x p(v) \sigma_{\bar{A}B,v}^m) \\ &= \frac{1}{2} p(v) - \text{tr} (X'_A \otimes X'_B \rho_{AB}^m), \end{aligned} \quad (22)$$

with σ_x denoting the Pauli matrix $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$. In the last line of Eq. (22) we have defined the operators

$$\begin{aligned} X'_A &= \mathbb{1}_{A_1 \dots A_{l-1}} \otimes X_A \otimes \mathbb{1}_{A_{l+2} \dots A_m}, \\ X'_B &= \frac{1}{2} F_v^{B\dagger} \sigma_x F_v^B \\ &= \frac{1}{4} (|2l-1\rangle\langle 2l+1| + |2l+1\rangle\langle 2l-1|), \end{aligned} \quad (23)$$

with $X_A = F_v^{A\dagger} \sigma_x F_v^A = |01\rangle\langle 10| + |10\rangle\langle 01|$.

Similar arguments apply to the cases where Bob announces subsequent even outcome pairs or the special instances at the borders of the blocks. We find that the averaged phase error $\bar{\delta} = \sum_{v \in \mathcal{V}_c} p(v)\delta_v$ can be written as

$$\bar{\delta} = \frac{1}{2} \sum_{v \in \mathcal{V}_c} p(v) - \text{tr} (X_{\bar{\delta}} \rho_{AB}^m), \quad (24)$$

with an operator $X_{\bar{\delta}} = \sum_{l=1}^m X_{A;l} \otimes X_{B;l}$. Here $X_{A;l}$ denotes the operator composed by the previously defined

X_A acting on qubits l and $l + 1$ and the identity operator acting on the remaining qubits ($l = m$ means the first and last qubit). On Bob's side the operators $X_{B;l}$ are given by

$$\begin{aligned} X_{B;l} &= \frac{1}{4} (|2l-1\rangle\langle 2l+1| + |2l+1\rangle\langle 2l-1| \\ &\quad + |2l\rangle\langle 2l+2| + |2l+2\rangle\langle 2l|), \end{aligned} \quad (25)$$

with addition being carried out modulo $2m$.

Channel model.—In this section we present the employed channel model of the COW experiment used in our numerical simulations. Note, however, that the results presented in this article can be applied as well to any other quantum channel, as they only depend on the observed detection probabilities in both the data and monitoring lines.

In particular, we characterize the losses in the channel with a BS of transmittance η_{channel} . This parameter can be related with a transmission distance d measured in km for the given QKD scheme as

$$\eta_{\text{channel}} = 10^{-\frac{\alpha d}{10}}, \quad (26)$$

where α represents the loss coefficient of the channel (*e.g.*, an optical fiber) measured in dB/km. Together with the efficiency of the detectors the overall system transmittance is given by

$$\eta_{\text{sys}} = \eta_{\text{channel}} \eta_{\text{det}}. \quad (27)$$

The total system loss in dB is used as the x-axis in the secret key rate figures, *i.e.*, $-10 \log_{10} \eta_{\text{sys}}$.

The channel misalignment is parametrized with an error probability e_d that a signal hits Bob's detectors in the wrong time slot within the same bit. For simplicity, we assume that e_d is a constant independent of the distance and we use $e_d = 1\%$ for simulation purposes. This effect is modelled by a completely positive trace-preserving map Φ that incoherently flips the signal states within the same bit slot as $|0, \sqrt{\eta_{\text{sys}}} \alpha\rangle \mapsto |\sqrt{\eta_{\text{sys}}} \alpha, 0\rangle$ and $|\sqrt{\eta_{\text{sys}}} \alpha, 0\rangle \mapsto |0, \sqrt{\eta_{\text{sys}}} \alpha\rangle$ with probability e_d . Here we consider that the input signals have been already affected by system losses. We have, therefore, that whenever Alice sends to Bob a corresponding COW signal state with coherent state $|\alpha\rangle$ in temporal mode d , the probability that Bob observes a single photon detection event in this mode only (within the whole signal block) is given by

$$\begin{aligned} p_d^{\text{correct}} &= \text{tr} \{ \Lambda_s [\Phi^{\otimes m}(\rho_{\text{loss}}^m)] M_d \} = \epsilon (1 - \epsilon)^{2m-1} e^{-\eta_{\text{sys}} \lambda} \\ &\quad + (1 - \epsilon)^{2m} (1 - e_d) \eta_{\text{sys}} \mu e^{-\eta_{\text{sys}} \lambda}, \end{aligned} \quad (28)$$

where ρ_{loss}^m represents the output signal of the BS characterizing the total system loss, $\mu = \alpha^2$, and $\lambda = m\mu$. Similarly, when Alice sends to Bob a vacuum state in temporal mode d Bob can observe a single photon detection event in this mode only with probability

$$\begin{aligned} p_d^{\text{error}} &= \epsilon (1 - \epsilon)^{2m-1} e^{-\eta_{\text{sys}} \lambda} \\ &\quad + (1 - \epsilon)^{2m} e_d \eta_{\text{sys}} \mu e^{-\eta_{\text{sys}} \lambda}. \end{aligned} \quad (29)$$

The total probability that Bob observes an inconclusive detection event in the data line is then given by

$$p_{\text{inc}} = 1 - m(p_d^{\text{correct}} + p_d^{\text{error}}). \quad (30)$$

In the monitoring line we include an additional misalignment effect that reduces further the interferometric visibility. In particular, we assume that whenever two equal coherent states interfere at a 50 : 50 BS then the outcome signal can exit the BS through the wrong output port with error probability e_m . In our simulations we use $e_m = 0.5\%$. Here we distinguish two possible scenarios, depending on whether the signals which interfere at the BS were prepared by Alice in the same quantum state or not. Let us assume that the first signal corresponds to bit i_l while the later to bit i_{l+1} . That is, Bob interferes modes $2l - 1, 2l + 1$ and, at the same time, $2l, 2l + 2$.

Let us consider first the situation where both signals were generated in the same state $|0, \alpha\rangle$. In this scenario, we find that Bob observes a single photon detection event in temporal mode $2l - 1$ only (and no click in the remaining modes of the block) with probability

$$\begin{aligned} p_{2l-1,+} &= \epsilon(1 - \epsilon)^{2m-1}e^{-\eta_{\text{sys}}\lambda} + (1 - \epsilon)^{2m}\eta_{\text{sys}}\mu e^{-\eta_{\text{sys}}\lambda} \\ &\quad \times [2(1 - e_d)^2(1 - e_m) + e_d(1 - e_d)], \\ p_{2l-1,-} &= \epsilon(1 - \epsilon)^{2m-1}e^{-\eta_{\text{sys}}\lambda} + (1 - \epsilon)^{2m}\eta_{\text{sys}}\mu e^{-\eta_{\text{sys}}\lambda} \\ &\quad \times [2(1 - e_d)^2e_m + e_d(1 - e_d)], \end{aligned} \quad (31)$$

where the superscript \pm indicates whether the single excitation is registered in the bright (D_+) or in the dark

(D_-) detector of the monitoring line. Similarly, we have that the probability that Bob sees a single photon detection in temporal mode $2l$ only is given by

$$\begin{aligned} p_{2l,+} &= \epsilon(1 - \epsilon)^{2m-1}e^{-\eta_{\text{sys}}\lambda} + (1 - \epsilon)^{2m}\eta_{\text{sys}}\mu e^{-\eta_{\text{sys}}\lambda} \\ &\quad \times [2e_d^2(1 - e_m) + e_d(1 - e_d)], \\ p_{2l,-} &= \epsilon(1 - \epsilon)^{2m-1}e^{-\eta_{\text{sys}}\lambda} + (1 - \epsilon)^{2m}\eta_{\text{sys}}\mu e^{-\eta_{\text{sys}}\lambda} \\ &\quad \times [2e_d^2e_m + e_d(1 - e_d)]. \end{aligned} \quad (32)$$

The case where both signals were generated in the same state $|\alpha, 0\rangle$ is completely analogous. One only needs to interchange Eqs. (31) and (32).

Finally, let us consider the situation where both signals are prepared in a different quantum state. In this scenario the probabilities are given by

$$\begin{aligned} p_{2l-1,+} &= p_{2l,+} \\ &= \epsilon(1 - \epsilon)^{2m-1}e^{-\eta_{\text{sys}}\lambda} + (1 - \epsilon)^{2m}\eta_{\text{sys}}\mu e^{-\eta_{\text{sys}}\lambda} \\ &\quad \times \left[2e_d(1 - e_d)(1 - e_m) + \frac{1 + 2e_d^2 - 2e_d}{2} \right], \end{aligned} \quad (33)$$

and

$$\begin{aligned} p_{2l-1,-} &= p_{2l,-} \\ &= \epsilon(1 - \epsilon)^{2m-1}e^{-\eta_{\text{sys}}\lambda} + (1 - \epsilon)^{2m}\eta_{\text{sys}}\mu e^{-\eta_{\text{sys}}\lambda} \\ &\quad \times \left[2e_d(1 - e_d)e_m + \frac{1 + 2e_d^2 - 2e_d}{2} \right]. \end{aligned} \quad (34)$$